The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

SUBJECT:
Multiple Vulnerabilities in PHP Could Allow For Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in PHP, the most severe of which could allow an attacker to execute arbitrary code, with failed exploit attempts potentially leading to denial of service conditions. PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications. Successfully exploiting these issues could allow remote attackers to execute arbitrary code in the context of the affected application.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild. There is known proof-of-concept code for these vulnerabilities.

SYSTEMS AFFECTED:
- PHP 5 prior to 5.5.37
- PHP 5 prior to 5.6.23
- PHP 7 prior to 7.0.8

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

PHP has released updates that address multiple vulnerabilities, the most severe of which could allow for arbitrary code execution. These vulnerabilities include:

Prior to 5.5.37

- Fixed bug #72268 (Integer Overflow in nl2br()).
- Fixed bug #72275 (Integer Overflow in json_encode()/json_decode()/ json_utf8_to_utf16()).
- Fixed bug #72400 (Integer Overflow in addcslashes/addslashes).
- Fixed bug #72403 (Integer Overflow in Length of String-typed ZVAL).
- Fixed bug #66387 (Stack overflow with imagefilltoborder) (CVE-2015-8874).
- Fixed bug #72298 (pass2_no_dither out-of-bounds access).
- Fixed bug #72339 (Integer Overflow in _gd2GetHeader() resulting in heap overflow).
- Fixed bug #72407 (NULL Pointer Dereference at _gdScaleVert).
- Fixed bug #72446 (Integer Overflow in gdImagePaletteToTrueColor() resulting in heap overflow).
- Fixed bug #72402 (_php_mb_regex_ereg_replace_exec - double free).
- Fixed bug #72455 (Heap Overflow due to integer overflows).
- Fixed bug #72262 (int/size_t confusion in SplFileObject::fread).
- Fixed bug #72433 (Use After Free Vulnerability in PHP's GC algorithm and unserialize).
- Fixed bug #72340 (Double Free Courruption in wddx_deserialize).
- Fixed bug #72434 (ZipArchive class Use After Free Vulnerability in PHP's GC algorithm and unserialize).

Prior to 5.6.23

- Fixed bug #72275 (Integer Overflow in json_encode()/json_decode()/ json_utf8_to_utf16()).
- Fixed bug #72400 (Integer Overflow in addcslashes/addslashes).
- Fixed bug #72403 (Integer Overflow in Length of String-typed ZVAL).
- Fixed bug #72298 (pass2_no_dither out-of-bounds access).
- Fixed bug #72337 (invalid dimensions can lead to crash).
- Fixed bug #72339 (Integer Overflow in _gd2GetHeader() resulting in heap overflow).
- Fixed bug #72407 (NULL Pointer Dereference at _gdScaleVert).
- Fixed bug #72446 (Integer Overflow in gdImagePaletteToTrueColor() resulting in heap overflow).
- Fixed bug #70484 (selectordinal doesn't work with named parameters).
- Fixed bug #72402 (_php_mb_regex_ereg_replace_exec - double free).
- Fixed bug #72455 (Heap Overflow due to integer overflows).
- Fixed bug #72140 (segfault after calling ERR_free_strings()).
- Fixed bug #72321 (invalid free in phar_extract_file()).
- Fixed bug #72262 (int/size_t confusion in SplFileObject::fread).
- Fixed bug #72433 (Use After Free Vulnerability in PHP's GC algorithm and unserialize).
- Fixed bug #72340 (Double Free Courruption in wddx_deserialize).
- Fixed bug #72434 (ZipArchive class Use After Free Vulnerability in PHP's GC algorithm and unserialize).

Prior to 7.0.8

- Fixed bug #72218 (If host name cannot be resolved then PHP 7 crashes).
- Fixed bug #72221 (segfault, past-the-end access).
- Fixed bug #72268 (Integer Overflow in nl2br()).
- Fixed bug #72275 (Integer Overflow in json_encode()/json_decode()/ json_utf8_to_utf16()).

- Fixed bug #72400 (Integer Overflow in addcslashes/addslashes).
- Fixed bug #72403 (Integer Overflow in Length of String-typed ZVAL).
- Fixed bug #72308 (fastcgi_finish_request and logging environment variables).
- Fixed bug #72298 (pass2_no_dither out-of-bounds access).
- Fixed bug #72337 (invalid dimensions can lead to crash) (Pierre)Fixed bug #72339 (Integer Overflow in gd2GetHeader() resulting in heap overflow).
- Fixed bug #72407 (NULL Pointer Dereference at _gdScaleVert).
- Fixed bug #64524 (Add intl.use_exceptions to php.ini-*).
- Fixed bug #72402 (_php_mb_regex_ereg_replace_exec - double free).
- Fixed bug #72455 (Heap Overflow due to integer overflows).
- Fixed bug #72143 (preg_replace uses int instead of size_t).
- Fixed bug #71573 (Segfault (core dumped) if paramno beyond bound).
- Fixed bug #72294 (Segmentation fault/invalid pointer in connection with pgsql_stmt_dtor).
- Fixed bug #72284 (phpdbg fatal errors with coverage).
- Fixed bug #72195 (pg_pconnect/pg_connect cause use-after-free).
- Fixed bug #72197 (pg_lo_create arbitrary read).
- Fixed bug #72262 (int/size_t confusion in SplFileObject::fread).
- Fixed bug #72433 (Use After Free Vulnerability in PHP's GC algorithm and unserialize).
- Fixed bug #72017 (range() with float step produces unexpected result).
- Fixed bug #72193 (dns_get_record returns array containing elements of type 'unknown').
- Fixed bug #72229 (Wrong reference when serialize/unserialize an object).
- Fixed bug #72300 (ignore_user_abort(false) has no effect).
- Fixed bug #72206 (xml_parser_create/xml_parser_free leaks mem).
- Fixed bug #72155 (use-after-free caused by get_zval_xmlrpc_type).
- Fixed bug #72340 (Double Free Courruption in wddx_deserialize).
- Fixed bug #72258 (ZipArchive converts filenames to unrecoverable form).
- Fixed bug #72434 (ZipArchive class Use After Free Vulnerability in PHP's GC algorithm and unserialize).

Successfully exploiting these issues could allow remote attackers to execute arbitrary code in the context of the affected application. Failed exploitation could result in a denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade to the latest version of PHP immediately, after appropriate testing.
- Apply the principle of Least Privilege to all systems and services.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to only those required.

REFERENCES:

PHP:
http://php.net/ChangeLog-5.php#5.5.37
http://php.net/ChangeLog-5.php#5.6.23

http://php.net/ChangeLog-7.php#7.0.8

https://bugs.php.net/bug.php?id=66387

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/